REMARKS

The Examiner has objected to the specification. Such objections have been overcome in view of the clarifications made hereinabove to the specification.

The Examiner has objected to the claims. Such objections have been overcome in view of the clarifications made hereinabove to the claims.

The Examiner has rejected Claims 1-21 under 35 U.S.C. 103(a) as being unpatentable over Menezes et al., Handbook of Applied Cryptography. Applicant respectfully disagrees with this rejection.

Specifically, the Examiner admits that Menezes fails to explicitly disclose applicant's claimed:

"sending a second message from the second node to a key distribution center, wherein the second message includes a first node identifier for the first node, a second node identifier for the second node, and a message authentication code created using a second node key belonging to the second node;

recreating the second node key at the key distribution center, wherein the second node key was previously created using the second node identifier and a secret key known only to the key distribution center;

verifying at the key distribution center the message authentication code in the second message using the second node key; and

if the message authentication code is verified" (emphasis added).

The Examiner continues by arguing that "Menezes discloses both MACs (see page 361, below definition 9.77) and identity-based keying (page 561, section 13.4.3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the key distribution protocol by including the use of a

MAC, in order to provide data origin authentication and data integrity ... and by including identity-based keying, in order to prevent forgery and impersonation."

Applicant respectfully disagrees with such assertion. Even if Menezes discloses both MACs and identity-based keying, such disclosure still fails to meet the claim language surrounding such the MAC and second node key, in applicant's claims. See, for example, the limitations noted below that show a unique context in which applicant's MAC and second node key are used:

"sending a second message from the second node to a key distribution center, wherein the second message includes a first node identifier for the first node, a second node identifier for the second node, and a message authentication code created using a second node key belonging to the second node;

recreating the second node key at the key distribution center, wherein the second node key was previously created using the second node identifier and a secret key known only to the key distribution center;

verifying at the key distribution center the message authentication code in the second message using the second node key; and

if the message authentication code is verified" (emphasis added).

Further, it would simply be unobvious to modify Menezes to meet applicant's claim limitations noted above, especially in view of the numerous advantages provided by such claim limitations (when taken in combination with the remaining claim elements).

Specifically, as noted in paragraph [0005] of the originally filed specification, applicant's claimed invention provides a particular advantage over key distribution schemes such Kerberos in that database updates are not required for unfamiliar participants. Since the technique relied upon by Menezes is analogous to Kerberos, it explicitly lacks (and even *teaches away* from) any sort of similar advantage. For these

reasons, applicant contends that it would simply not be obvious to modify Menezes to meet applicant's claim limitations noted above.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since the prior art reference fails to teach or suggest all the claim limitations, and it would not be obvious to modify the prior art reference, as suggested by the Examiner. A notice of allowance or a specific prior art showing of each of the foregoing limitations, in combination with the remaining claim elements, is respectfully requested.

Despite the foregoing stark differences and in the spirit of expediting the prosecution of the present application, applicant now claims the following in each of the independent claims:

"wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar."

Again, with applicant's claimed invention, database updates are at least partially not required for unfamiliar participants. A notice of allowance or a specific prior art showing of such feature, in combination with the remaining claim elements, is respectfully requested.

It is further noted that the Examiner's rejection with respect to applicant's dependent claims is further replete with deficiencies. Specifically, with respect to Claim 2 et al., the Examiner admits that the protocol in Menezes "does not explicitly disclose recreating a first node key previously created using the first node identifier and the secret key." The Examiner goes on to argue that "Menezes discloses identity-based keying" and further "although the protocol does not explicitly disclose the use of a hash value in the messages for verification, Menezes discloses that hash values can be used for verification of data." The Examiner then concludes that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the key distribution protocol by including the use of a hash, in order to provide data integrity."

Again, for the reasons set forth hereinabove, not only are applicant's claims not met, but it would be *unobvious* to modify Menezes to meet applicant's claims. Only applicant teaches such specific flow for the purpose of providing a technique wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar.

It further appears that the rejection of the remaining claims is also replete with deficiencies. Again, a notice of allowance or a specific prior art showing of each of the foregoing limitations, in combination with the remaining claim elements, is respectfully requested.

To this end, all of the pending independent claims are deemed allowable, along with any dependent claims dependent therefrom.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are

enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P254).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100